

## **Welcome to the PIA for FY 2011!**

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

### **Directions:**

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: [http://vaww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp)

### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

### **Definition of PII (Personally Identifiable Information)**

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

### **Macros Must Be Enabled on This Form**

**Microsoft Office 2003:** To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

**Microsoft Office 2007:** To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

**Final Signatures**

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

**Privacy Impact Assessment Uploaded into SMART**

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to [christina.pettit@va.gov](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

Program or System Name: Region 2>VHA>VISN23>CENTRAL IOWA HCS>  
OMB Unique System / Application / Program Identifier (AKA: UPID #):

Description of System/ Application/ Program: Local Area Network - Central Iowa Health Car supporting mission critical and other systems Applications and devices within the LAN supp decision support, and education.

Facility Name: Central Iowa HCS

Title:	Name:	Phone:
Privacy Officer:	Jessica Carper	515-699-5999 x1
Information Security Officer:	Jon Cruikshank	515-699-5740
System Owner/ Chief Information Officer:	Stan R. Bush	612-467-1200
Information Owner:	Donald Cooper	515-699-5850
Other Titles:		

Person Completing Document:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)

Date Approval To Operate Expires:

What specific legal authorities authorize this program or system:

What is the expected number of individuals that will have their PII stored in this system:

Identify what stage the System / Application / Program is at:

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

Is there an authorized change control process which documents any changes to existing applications or systems?

If No, please explain:

Has a PIA been completed within the last three years?

Date of Report (MM/YYYY):

**Please check the appropriate boxes and continue to the next TAB and complete the remaining**

- ☐ Have any changes been made to the system since the last PIA?
- ☒ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

☒ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please only complete TAB 2

---

LAN

029-00-02-00-01-1120-00

The System uses the Local Area Network (LAN) as a General Support System, necessary to conduct day to day operations within the medical center. It supports numerous areas, including medical imaging, supply management,

---

Email:

[jessica.carper@va.gov](mailto:jessica.carper@va.gov)

[jon.cruikshank@va.gov](mailto:jon.cruikshank@va.gov)

[stan.bush@va.gov](mailto:stan.bush@va.gov)

[donald.cooper@va.gov](mailto:donald.cooper@va.gov)

[Jon Cruikshank, Lydia Wynes, Jessica Carper](#)

02/2008

08/2011

---

Title 38 U.S.C. section 7301(a) and Title 38 U.S.C. 501(b) and 304  
100,000  
Operations/Maintenance

12 years

Yes

Yes

---

02/2011

**g questions on this form.**

Employees, contractors, or others performing work for  
basis of name, unique identifier, symbol, or

& 12. ( See Comment for Definition of PII)

## (FY 2011) PIA: System of Records

---

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

---

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):
  2. Name of the System of Records:
  3. Location where the specific applicable System of Records Notice may be accessed (include the URL):
- 

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

---

Does the System of Records Notice require modification or updating?

---

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

---

Yes
24VA19; 79VA19
Patient medical record - VA
<a href="http://vaww.vhaco.va.gov/privacy/systemofrecords.htm">http://vaww.vhaco.va.gov/privacy/systemofrecords.htm</a>
Yes
No
<b><i>(Please Select Yes/No)</i></b>
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes



## (FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	Benefits, Health Care	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Benefits, Health Care	Verbal & Written	Verbal & Written
Service Information	ALL	Health Care	Verbal & Written	Verbal & Written
Medical Information	ALL	Health Care	Verbal & Written	Verbal & Written
Criminal Record Information	ALL	Benefits	Verbal & Automatic	Written
Guardian Information	Paper & Electronic	Benefits	Verbal & Written	Verbal & Written
Education Information	ALL	Benefits	Verbal & Written	Verbal & Written
Benefit Information	ALL	Benefits	Verbal & Written	Verbal & Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information	Yes	Veteran	Mandatory	

Medical Information	Yes	Veteran	Mandatory
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory
Guardian Information	Yes	Veteran	Mandatory
Education Information	Yes	Veteran	Mandatory
Benefit Information	Yes	Veteran	Mandatory
Other (Explain)			
Other (Explain)			
Other (Explain)			

## (FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization		No			
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System		No			
Other Project / System		No			
Other Project / System		No			

## (FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	HINQ, BIRLS, VIS for eligibility Data
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

## (FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
if yes, please check all that apply:	<input type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input checked="" type="checkbox"/> Other (Please Explain)

Describe process for authorizing access to this data.

Answer: BAA or Authorization to release PII

## (FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify: N/A

Explain how collected data are limited to required elements:

Answer: Data is collected from VA forms and clinical procedures for all necessary data. The website's privacy statements certify that PII provided by the veteran will be used only in connection with VA programs and services or for such purposes as are described at the point of collection. Forms & applications that are manually completed are scanned for storing and transmission.

How is data checked for completeness?

Answer: Information is entered and compared to the answers given by the individual. Audits are performed by responsible departments to ensure the information is complete and accurate.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Information stored on the LAN is historical data & is not changed without change control documentation when changes are required. Policies are in place that require form completion for name or service changes

How is new data verified for relevance, authenticity and accuracy?

Answer: The patient is required to provide updated information upon registration for each visit. If a change is needed the registrar completes the change

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer: N/A

## (FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

Explain why the information is needed for the indicated retention period?

Answer: Kept per VA Records Control Schedule 10-1.

What are the procedures for eliminating data at the end of the retention period?

Answer: When records are retired they are sent to NEOSHA or Destroyed as mandated in records control schedule, Electronic final version of patient medical records are destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1

Where are these procedures documented?

Answer: VA Directive 6500; 44 U.S.C Chapter 22, VHA Handbook 1907.1, VA Handbook 6300; Records Control Schedule 10-1

How are data retention procedures enforced?

Answer: VA Records Control Schedule 10-1: Records Management Responsibilities. The Chief of HIMS has developed the policies and procedures for effective and efficient records management throughout the hospital. Record liaison officers have been established for every department and have gone through the records management training.

---

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

---

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer: Yes

---

### **(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)**

---

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer: N/A

---

## (FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: The system is compliant with FISMA.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure          | <input checked="" type="checkbox"/> Data Disclosure                       | <input checked="" type="checkbox"/> Hardware Failure   |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss                   | <input checked="" type="checkbox"/> Identity Theft     |
| <input checked="" type="checkbox"/> Blackmail                         | <input checked="" type="checkbox"/> Denial of Service Attacks             | <input checked="" type="checkbox"/> Malicious Code     |
| <input checked="" type="checkbox"/> Bomb Threats                      | <input type="checkbox"/> Earthquakes                                      | <input checked="" type="checkbox"/> Power Loss         |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery         | <input checked="" type="checkbox"/> Eavesdropping/Interception            | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow                   | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes  |
| <input checked="" type="checkbox"/> Communications Loss               | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input checked="" type="checkbox"/> Substance Abuse    |
| <input checked="" type="checkbox"/> Computer Intrusion                | <input checked="" type="checkbox"/> Flooding/Water Damage                 | <input checked="" type="checkbox"/> Theft of Assets    |
| <input checked="" type="checkbox"/> Computer Misuse                   | <input checked="" type="checkbox"/> Fraud/Embezzlement                    | <input checked="" type="checkbox"/> Theft of Data      |
| <input checked="" type="checkbox"/> Data Destruction                  |   | <input checked="" type="checkbox"/> Vandalism/Rioting  |

Answer: (Other Risks)

---

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control                                       | <input checked="" type="checkbox"/> Contingency Planning              | <input checked="" type="checkbox"/> Personnel Security                    |
| <input checked="" type="checkbox"/> Audit and Accountability                             | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Incident Response                 | <input checked="" type="checkbox"/> Risk Management                       |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |   |
| <input checked="" type="checkbox"/> Configuration Management                             | <input checked="" type="checkbox"/> Media Protection                  |   |

Answer: (Other Controls)

---

## PIA: PIA Assessment

---

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: Review privacy notices, data protection methods and review security controls.

---

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**



The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.



The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.



The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

---

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?  
**(Choose One)**



The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.



The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.



The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

---

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**



The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.



The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.



The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

---

---

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

---

*Please add additional controls:*

---



(FY 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

## (FY 2011) PIA: VBA Minor Applications

### Which of these are sub-components of your system?

X Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	X BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
X ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	x Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	x Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	X Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	x Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
X BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
X C&P Payment System	X Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	x Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	x Enterprise Wireless Messaging System (Blackberry)
X Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
X Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	x Personnel and Accounting Integrated Data and Fee Basis (PAID)
X INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	X Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
X MUSE	Mental Health Asisstant	Service Member Records Tracking System
X Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
X RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	X VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
x Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

VBA Data Warehouse	X Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?
---

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?
---

Name Description Comments Is PII collected by this min or application? Does this minor application store PII? If yes, where? Who has access to this data?
---

**(FY 2011) PIA: VISTA Minor Applications**

**Which of these are sub-components of your system? Central Iowa**

x ASISTS	x Beneficiary Travel	x Accounts Receivable	x Adverse Reaction Tracking
x Bed Control	x Care Management	x ADP Planning (PlanMan)	x Authorization/ Subscription
CAPRI	x Care Tracker	x Bad Code Med Admin	x Auto Replenishment/ Ward Stock
x CMOP	x Clinical Reminders	x Clinical Case Registries	x Automated Info Collection Sys
x Dental	x CPT/ HCPCS Codes	x Clinical Procedures	x Automated Lab Instruments
x Dietetics	x DRG Grouper	x Consult/ Request Tracking	x Automated Med Info Exchange
x Fee Basis	x DSS Extracts	x Controlled Substances	x Capacity Management - RUM
x GRECC	x Education Tracking	x Credentials Tracking	x Capacity Management Tools
x HINQ	x Engineering	x Discharge Summary	x Clinical Info Resource Network
x IFCAP	x Event Capture	x Drug Accountability	x Clinical Monitoring System
x Imaging	x Extensible Editor	x EEO Complaint Tracking	x Enrollment Application System
x Kernal	x Health Summary	x Electronic Signature	x Equipment/ Turn-in Request
x Kids	x Incident Reporting	x Event Driven Reporting	x Gen. Med.Rec. - Generator
x Lab Service	x Intake/ Output	x External Peer Review	x Health Data and Informatics
x Letterman	x Integrated Billing	x Functional Independence	x ICR - Immunology Case Registry
x Library	x Lexicon Utility	x Gen. Med. Rec. - I/O	x Income Verification Match
x Mailman	x List Manager	x Gen. Med. Rec. - Vitals	x Incomplete Records Tracking
x Medicine	x Mental Health	x Generic Code Sheet	x Interim Mangement Support
x MICOM	x MyHealthEVet	x Health Level Seven	x Master Patient Index Vista
x NDBI	x National Drug File	x Hospital Based Home Care	x Missing Patient Reg (Original) A4EL
x NOIS	x Nursing Service	x Inpatient Medications	x Order Entry/ Results Reporting
x Oncology	x Occurrence Screen	x Integrated Patient Funds	x PCE Patient Care Encounter
x PAID	x Patch Module	x MCCR National Database	x Pharmacy Benefits Mangement
x Prosthetics	x Patient Feedback	x Minimal Patient Dataset	x Pharmacy Data Management
x QUASER	x Police & Security	x National Laboratory Test	x Pharmacy National Database
x RPC Broker	x Problem List	x Network Health Exchange	x Pharmacy Prescription Practice
x SAGG	x Progress Notes	x Outpatient Pharmacy	x Quality Assurance Integration
x Scheduling	x Record Tracking	x Patient Data Exchange	x Quality Improvement Checklist
x Social Work	x Registration	x Patient Representative	x Radiology/ Nuclear Medicine
x Surgery	x Run Time Library	x PCE Patient/ HIS Subset	x Release of Information - DSSI
x Toolkit	x Survey Generator	x Security Suite Utility Pack	x Remote Order/ Entry System
x Unwinder	x Utilization Review	x Shift Change Handoff Tool	x Utility Management Rollup
x VA Fileman	x Visit Tracking	x Spinal Cord Dysfunction	x CA Verified Components - DSSI
x VBECS	x VistALink Security	x Text Integration Utilities	x Vendor - Document Storage Sys
x VDEF	x Women's Health	x VHS & RA Tracking System	x Visual Impairment Service Team ANRV
x VistALink		x Voluntary Timekeeping	x Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web		ENDSOFT		RAFT
		Enterprise Terminology Server &		RALS
A4P	X	VHA Enterprise Terminology		
		Services	X	

## (FY 2011) PIA: Final Signatures

Facility Name:

Region 2>VHA>VISN23>CENTRAL IOWA HCS>LAN

Title:

Name:

Phone:

Email:

Privacy Officer:

Jessica Carper

515-699-5999 x9-4465

[jessica.carper@va.gov](mailto:jessica.carper@va.gov)

X

Jessica Carper  
Privacy Officer

Information Security Officer:

Jon Cruikshank

515-699-5740

[jon.cruikshank@va.gov](mailto:jon.cruikshank@va.gov)

X

Jon Cruikshank  
Information Security Officer

System Owner/ Chief Information Officer:

Stan Bush

612-467-1200

[stan.bush@va.gov](mailto:stan.bush@va.gov)

X

Stan Bush  
N23 Chief Information Officer

Information Owner:

Donald Cooper

515-699-5850

[donald.cooper@va.gov](mailto:donald.cooper@va.gov)

Other Titles:0

Date of Report:2/1/11  
OMB Unique Project Identifier029-00-02-00-01-1120-00

Project NameRegion 2>VHA>VISN23>CENTRAL  
IOWA HCS>LAN

0

0



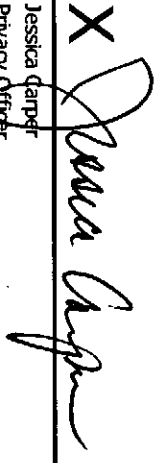
LAN


(FY 2011) PIA: Final Signatures

Facility Name: Region 2>VHA>VISN23>CENTRAL IOWA HCS>LAN

Title: Name: Phone: Email:

Privacy Officer: Jessica Carper 515-699-5999 x9-4465 jessica.carper@va.gov

X  3/17/11  
Jessica Carper  
Privacy Officer  
Information Security Officer: Jon Cruikshank 515-699-5740 jon.cruikshank@va.gov  
2/23/2011

X   
Jon Cruikshank  
Information Security Officer

System Owner/ Chief Information Officer: Stan Bush 612-467-1200 stan.bush@va.gov

X   
Stan Bush  
N23 Chief Information Officer  
Digitally signed by Stanley R. Bush  
DN: c=US, o=US Government, ou=Department of  
Veterans Affairs, ou=Internal Staff,  
0.9.2342.19200300.100.1.1=stan.bush@va.gov,  
cn=Stanley R. Bush  
Date: 2011.03.15 09:23:49 -05'00'

Information Owner: Donald Cooper 515-699-5850 donald.cooper@va.gov